특집 03

SSO based Security Management in Cloud Computing Environment

Jing Si Da · Youngmin Jung · Mokdong Chung
(Pukyong National University)

목 차

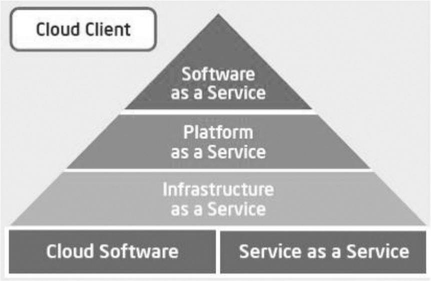
1. Introduction

Although the term "Cloud Computing" is based on a collection of many old and few new concepts in several research fields like Service-Oriented Architectures(SOA), distributed and grid computing as well as virtualization, it has created much interest in the last few years. This was a result of its huge potential for substantiating other technological advances while presenting a superior utilitarian advantage over the currently under-utilized resources deployed at data centers, security is the most important element in cloud computing environment, also there are different models in cloud computing, for example, cloud application, that's SaaS, thus we must consider all the elements in cloud computing environment, since cloud computing including so much. In this paper, we mention an approach to implement the security management in cloud computing environment, at the same time, we concern on the security aspect of SSO architecture in cloud computing environment.

2. Related Work

2.1 Cloud Computing Model Overview

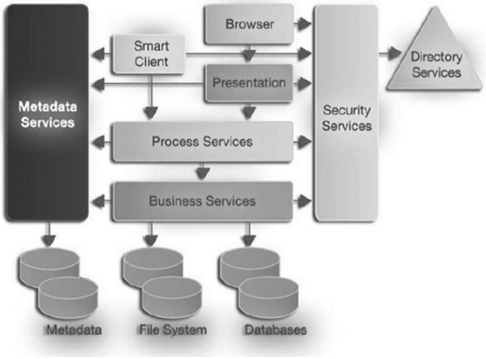
Cloud computing is an emerging computing technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. Cloud computing is broken down into three segments: "applications," "platforms," and "infrastructure." Each segment serves a different purpose and offers different products for businesses and individuals around the world. To promote the use of common definitions, Intel has developed a cloud computing taxonomy The taxonomy includes several established categories of cloud computing service, as shown in (Figure 1) [8].



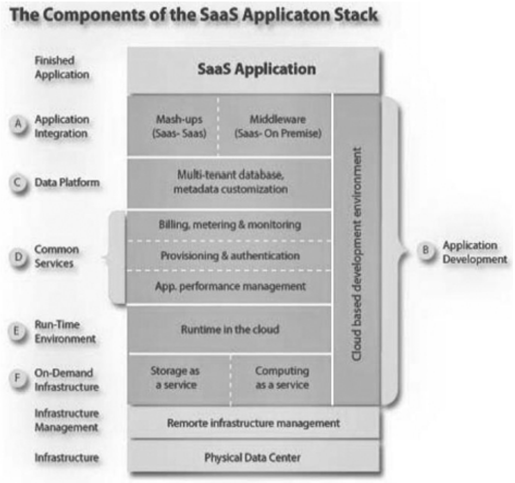
(Figure 1) Cloud Computing Taxonomy(Intel)[1]

2.2 SaaS (Software as a Service)

Software as a Service(SaaS) is a model of software deployment where an application is hosted as a service provided to customers across the Internet. (Figure 2) shows SaaS Architecture, including metadata services, security services components, software developed as a hosted services, the browser and process service access over directory service through security service. (Figure 3) shows SaaS Application Stack Components, from the top to end, application integration, data platform, common service run-time environment, on-demand infrastructure [15].



(Figure 2) Typical SaaS Architecture[15]


The Components of the SaaS Applicaton Stack
Finished Application
SaaS Application
A Application Integration
Mash-ups (Saas- Saas)
Middleware (Saas- On Premise)
C Data Platform
Multi-tenant database, metadata customization
D Common Services
Billing, metering & monitoring
Provisioning & authentication
App. performance management
E Run-Time Environment
Runtime in the cloud
F On-Demand Infrastructure
Storage as a service
Computing as a service
Cloud based development environment
B Application Development
Infrastructure Management
Remorte infrastructure management
Infrastructure
Physical Data Center

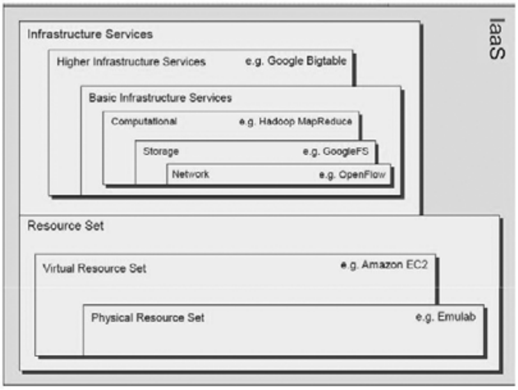
(Figure 3) SaaS Application Stack Components[15]

2.3 PaaS (Platform as a Service)

"Cloud computing" has dramatically changed how business applications are built and run. At its core, cloud computing eliminates the costs and complexity of evaluating, buying, configuring, and managing all the hardware and software needed for enterprise applications. Instead, these applications are delivered as a service over the Internet [10].

2.4 IaaS (Infrastructure as a Service)

Infrastructure as a Service(IaaS) is the delivery of computer infrastructure(typically a platform virtualization environment) as a service. It is an evolution of web hosting and virtual private server offerings. Infrastructure as a Service is an evolution of web hosting and virtual private server offerings. (Figure 4) shows the Architecture of Infrastructure as a Service, practically, the infrastructure services include storage, computational, network, database.

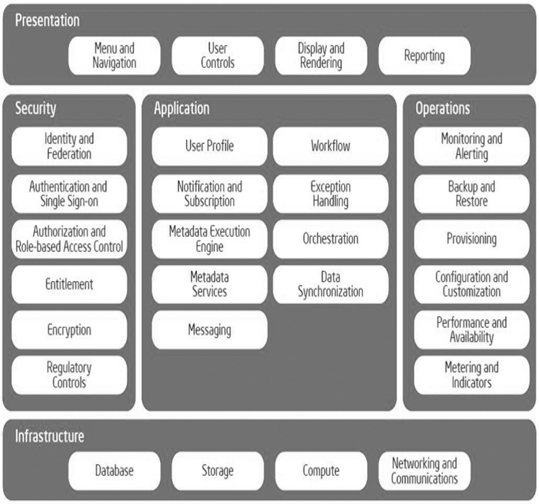


(Figure 4) Infrastructure as a Service Architecture[18]

3. Security Issues in Cloud Computing Environment

3.1 Architecting Software as a Service

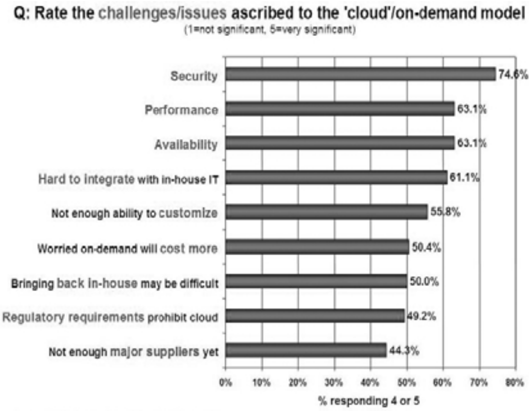
Many capabilities make up the SaaS architecture, A well-designed SaaS application has several key point, for instance, Multi-tenant efficient, Configurable, Configurable. (Figure 5) shows SaaS Architecture which was mix in presentation, security, application, operations, and infrastructure categories.



(Figure 5) SaaS Architecture[1]

3.2 Security Challenge in Cloud Computing Environment

There are so many issues in cloud computing environment, from the report of cloud computing, we find that there are 9 Challenges on the top, security is the most important item in this report, as shown in (Figure 6).

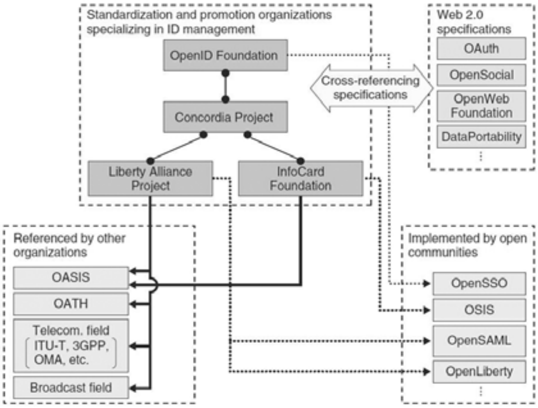


Source: IDC Enterprise Panel, August 2008 n=244

(Figure 6) Security Challenge in Cloud Computing Environment[6]

3.3 Identity Management(IdM)

Technologies for managing user identities across multiple web applications can be classified as either single sign-on(SSO) technologies or attribute exchange technologies. In the former, the authentication procedures for different applications(from various service providers) are aggregated by an authentication provider(identity provider) and services are provided to users on the basis of the authentication results issued by the identity provider. At the moment, the main SSO technologies are SAML(security assertion markup language) OpenID and Info Card and the main attribute exchange technology is ID-WSF(Web Services Framework). For each of these technologies (Figure 7), some industry groups have been set up to decide the specifications and encourage use of the technologies SAML, OpenID, and Info Card technologies are all chiefly targeted at IdM in web applications[4].


Standardization and promotion organizations specializing in ID management
OpenID Foundation
Concordia Project
Liberty Alliance Project
InfoCard Foundation
Cross-referencing specifications
Web 2.0 specifications
OAuth
OpenSocial
OpenWeb Foundation
DataPortability
Referenced by other organizations
OASIS
OATH
Telecom. field (ITU-T, 3GPP, OMA, etc.)
Broadcast field
Implemented by open communities
OpenSSO
OSIS
OpenSAML
OpenLiberty

(Figure 7) Groups Technologies Related to IdM[4]

4. SSO–based Security Issues and Analysis in Cloud Computing Environment

4.1 Risks and Security Vulnerabilities of SSO

As stated earlier, "The intent of Liberty version 1 is to make single sign-on to multiple sites substantially as secure as giving a name and password at each site. This is a strong argument for the user and the implementer to exercise care when using and implementing web technologies [21]. For example, it has a single authentication point, and it leads to a lockout of valid users, gradually, it causes an administrative bottleneck.

4.2 Security-based Access Control and Security Levels

4.2.1 Building Access and Alarms [19]

Interior doors can be controlled by the following methods:

A. Scheduling – The system can schedule general door openings and closings and/or access to individuals through keypads or card readers in advance on a regular schedule or for specific, one-time special events. Building alarms can sound locally and/or send a signal to Security and Fire Prevention Services. Some types of alarms are:

1) Security – including unscheduled or unexpected door openings, door propping, motion and heat detection, glass breaks.

2) Fire – these alarms are triggered by the sensors detecting smoke and/or heat.

3) Environmental – these alarms can be triggered by various causes such as temperature, moisture, etc.

4) Trouble/fault/hazard – these alarms detect problems with the device and send notification to the individuals monitoring alarms

4.2.2 Security Levels in Cloud Computing Environment

A. Server access security

B. Internet access security

C. Database access security

D. Data privacy security

E. Program access security [22]

4.3 SSO Support for Multi and Different Domain in Cloud Computing Environment

We will implement SSO and make it work in different scenarios.

A. SSO for parent and child application in the virtual sub-directory

B. SSO using different authorization credentials (username mapping)

C. SSO for two applications in two sub-domains of the same domain

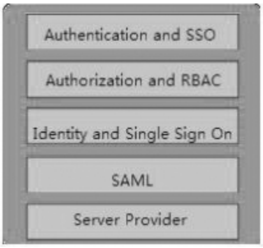
D. SSO when applications run under different versions of .NET

E. SSO for two applications in different domains.

F. SSO for mixed-mode authentication (Forms and Windows)

4.4 Security Components and Modules

The cloud security components add authentication, SAML Component and access control to applications, shown in (Figure 8). These Cloud Computing Security Components include Identity and Federation, Authentication and Single Sign-On, Authorization and Role-Based Access Control, Server Provider.

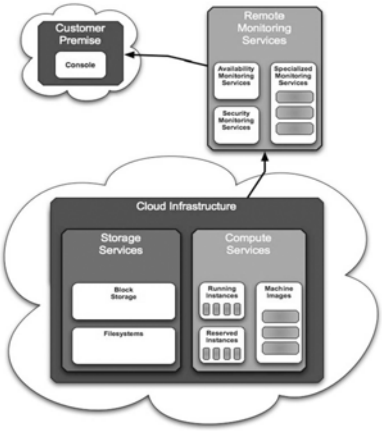


(Figure 8) Security Components and Modules in SaaS Environment[1]

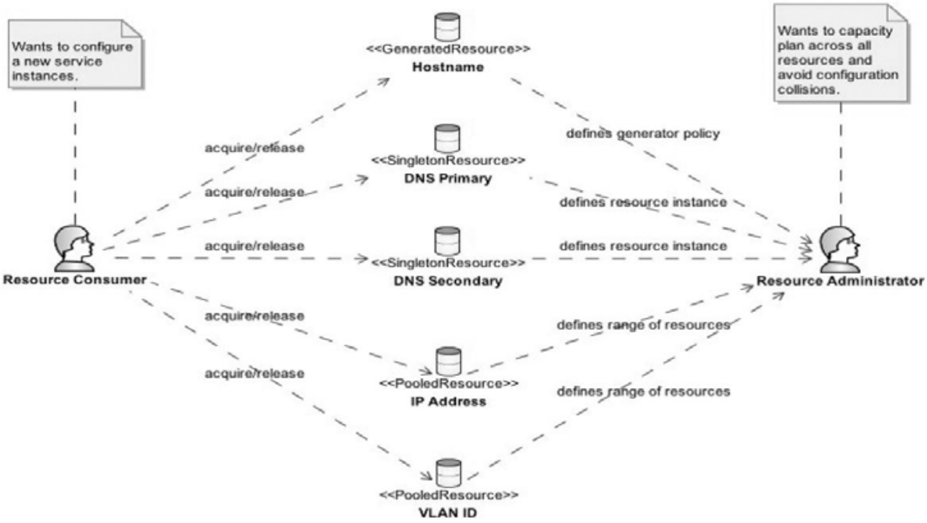
5. Security-Oriented SSO Architecture in Cloud Computing Environment

5.1 Existing Cloud Computing Patterns Combined with Software and Infrastructure

The existing patterns could combine software and infrastructure patterns to leverage cloud computing with Application. Pattern means that it can solve a problem that can be implemented in many ways to be applied to many sets of problems. Architecture means combine software and infrastructure to solve both functional and systemic problems. In this paper, we focus on how to combine these elements, there are 2 models in cloud computing environment, any way, we aim to embedded SSO into cloud computing environment, for instance, (Figure 9) shows A general method of monitoring service availability and performance from premises remote to cloud operations. This is a collection of patterns that involve monitoring of services in the cloud from a remote premise. If you want to manage resources or be a Administration of Cloud Resource, you can choose Cloud Resource Administration Pattern, as shown in (Figure 10), there are several resources that are consumed and released, In cloud, it's a large-scale environment, the complexity of these resources easily goes beyond paper or spreadsheet management, and requires an automated management system. The resource allocation manager is responsible for satisfying the resource requests.



(Figure 9) Monitoring Cloud Services Pattern[20]

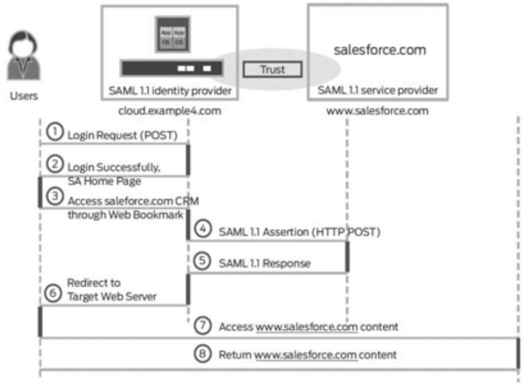


(Figure 10) Resources Administration Pattern[20]

5.2 SSO Use Cases in Cloud Computing Environment

5.2.1 SSO Integrating SaaS

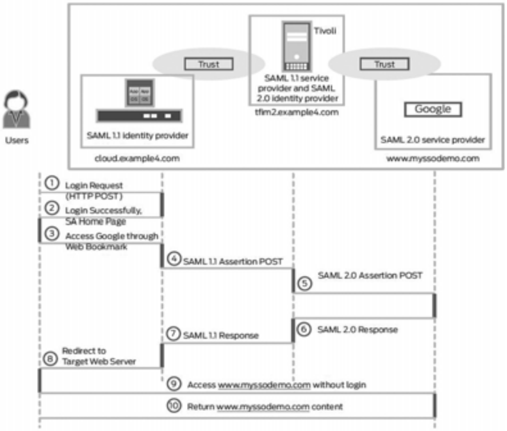
With the SAML-based SSO, the enterprise can integrate the SaaS on the public cloud into a remote access portal, managing authentication and authorization policy locally. (Figure 11) demonstrates that the user logging in on an SA Series appliance can access Salesforce.com's CRM business application without satisfying any additional credential challenges [5].


Users
SAML 1.1 identity provider
cloud.example4.com
Trust
salesforce.com
SAML 1.1 service provider
www.salesforce.com
① Login Request (POST)
② Login Successfully, SA Home Page
③ Access saleforce.com CRM through Web Bookmark
④ SAML 1.1 Assertion (HTTP POST)
⑤ SAML 1.1 Response
⑥ Redirect to Target Web Server
⑦ Access www.salesforce.com content
⑧ Return www.salesforce.com content

(Figure 11) SSO Integrating SaaS Case[5]

5.2.2 SSO Integrating Public Cloud Service

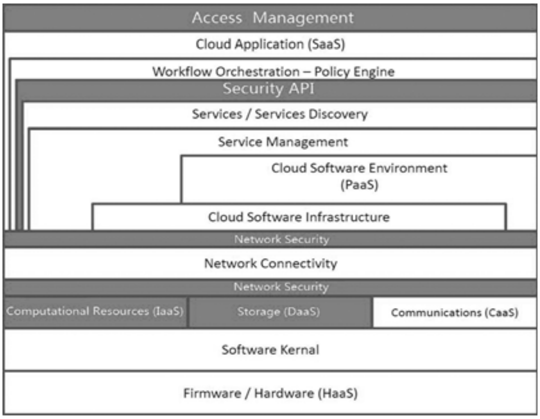
Through the SAML-based SSO, the enterprise can integrate the Platform as a Service(PaaS) with the remote access portal, having full control over PaaS authentication and authorization. (Figure 12) demonstrates that the user logging in on the SA Series can access Google applications such as Gmail and Google Calendar, without being required to fulfill additional credential challenges [5].


Tivoli
Trust
Trust
SAML 1.1 service provider and SAML 2.0 identity provider
tfim2.example4.com
Google
Users
SAML 1.1 identity provider
cloud.example4.com
SAML 2.0 service provider
www.myssodemo.com
① Login Request (HTTP POST)
② Login Successfully, SA Home Page
③ Access Google through Web Bookmark
④ SAML 1.1 Assertion POST
⑤ SAML 2.0 Assertion POST
⑥ SAML 2.0 Response
⑦ SAML 1.1 Response
⑧ Redirect to Target Web Server
⑨ Access www.myssodemo.com without login
⑩ Return www.myssodemo.com content

(Figure 12) Integrating Public Cloud Service[5]

5.3 Security Management based on SSO Architecture in Cloud Computing Environment

Security is the most important problem we face, there are several Identify Threats : "What attacks can be mounted? What other threats are there". There are an approach to secure cloud computing, in access management layer, use "Out of Band" authentication, Network Security layer, we use "Data in Motion" security, as shown in (Figure 12), the storage solution, DaaS maybe the best.


Access Management
Cloud Application (SaaS)
Workflow Orchestration – Policy Engine
Security API
Services / Services Discovery
Service Management
Cloud Software Environment (PaaS)
Cloud Software Infrastructure
Network Security
Network Connectivity
Network Security
Computational Resources (IaaS)
Storage (DaaS)
Communications (CaaS)
Software Kernal
Firmware / Hardware (HaaS)

(Figure 13) A Security Architecture Method of Cloud Computing[6]

5.3.1 Security Architecture Implementation

A. SSO Authentication Managements

Use the function that submit service requests from anywhere in the world to the Data Center and cloud to be process.

B. Cloud Application(SaaS)

SaaS applications expose services that can be accessed by on-premises applications or by other cloud applications. It is a Deployment/ Delivery model, for instant, hosted and managed by vendor, delivered across the internet.

C. Workflow Orchestration-Policy Engine

A workflow engine is a software application that manages and executes modeled computer processes. It is a key component in workflow technology and typically makes use of a database server. A workflow engine interprets events, such as documents submitted to a server or due dates expiring, and acts on them according to defined computer processes. The actions may be anything from saving the document in a document management system to issuing new work by sending an e-mail to users or escalating overdue work items to management. A workflow engine facilitates the flow of information, tasks, and events. Workflow engines may also be referred to as a Workflow Orchestration Engines [25].

D. Service Management

The service management acts as the interface between the Cloud service provider and customer. It requires the interaction of so many elements to support Resource management.

E. SSO Security API Support SAML

OASIS has completed SAML, a standard for exchanging authentication and authorization information between domains. SAML is designed to offer single sign on for both automatic and manual interactions between systems [23].

F. Cloud Software Environment(PaaS)

Cloud software environment deliver a computing platform, it is used to deploy applications. Platforms serve as an interface for users to access applications provided by partners or in some cases the customers.

G. Computational Resources(IaaS)

IaaS provides IT resources - processing power, storage, data center space, services, compliance - on-demand. The Key components (including Service level agreements, Utility computing billing, Platform virtualization environment for running client specified virtual machines, Computer hardware, Computer network, Internet connectivity) also have several Challenges, for instance, Old-fashioned network models, Multi tasking systems, Multi operating systems, Multi domains, Complex Networks, Security of network. Any way, if you design IaaS, you may need this advice: Security File System, Privilege Messaging mechanism and Compliance International Standard.

H. Network Security

Security is necessary that it may take the process of preventing and detecting unauthorized use of your computer. At the same time Prevention assessment help you to stop unauthorized users from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system.

I. Network Connection Security

A secured VPN internet connection not directly connection to the server as well this method can meet the demand of users.

J. DaaS (Data as a Service)

Data center allows customers collect this data from individuals or companies by providing immediate value back for these efforts, and storage is long-time preservation and multi application oriented, in all we should save storage space as much as possible and enhance the security level in storage layer.

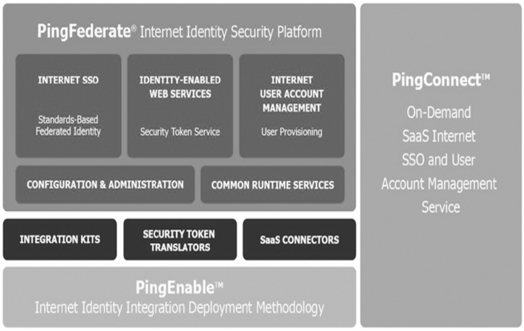
K. Communications(CaaS)

To meet accepted service requests sometimes SaaS delivery model can be applied to various communication services including contact center automation. This utility-like model for communications is often referred to as Communications as a Service(CaaS).

6. Existing SSO Solutions in Cloud Computing Environment

6.1 SSO Solution(Ping Identity)

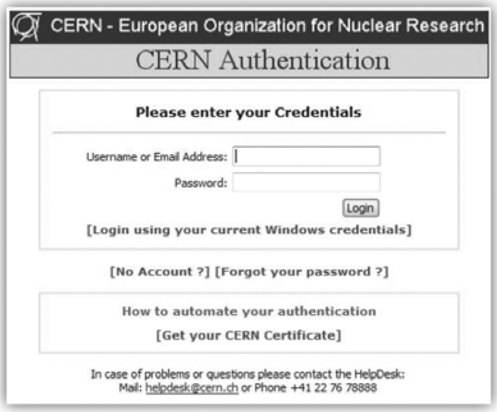
SSO Solution including Internet Identity Security software platform, a set of add-on modules, and external services. As shown in (Figure 14). PingConnect is the industry's first complete on-demand Internet SSO service for Software-as-a-Service applications. PingFederate is Ping Identity's award-winning federated identity software [9].


PingFederate® Internet Identity Security Platform
INTERNET SSO
Standards-Based Federated Identity
IDENTITY-ENABLED WEB SERVICES
Security Token Service
INTERNET USER ACCOUNT MANAGEMENT
User Provisioning
CONFIGURATION & ADMINISTRATION
COMMON RUNTIME SERVICES
INTEGRATION KITS
SECURITY TOKEN TRANSLATORS
SaaS CONNECTORS
PingEnable™
Internet Identity Integration Deployment Methodology
PingConnect™
On-Demand SaaS Internet SSO and User Account Management Service

(Figure 14) Pingidentity SSO Solution in SaaS Environment[9]

6.2 CERN Solution

Single Sign On(SSO) is a specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple software systems. CERN Single Sign On solution will simply allow users to authenticate using a single login/password pair or using a Certificate to increase security. It is very simple to implement authentication. Shown in (Figure 15), it's easy to login use CERN solution. The same authentication form will be used, completely unrelated to the calling application [7].


CERN - European Organization for Nuclear Research

CERN Authentication

Please enter your Credentials

Username or Email Address:

Password:

Login

[Login using your current Windows credentials]

[No Account ?] [Forgot your password ?]

How to automate your authentication

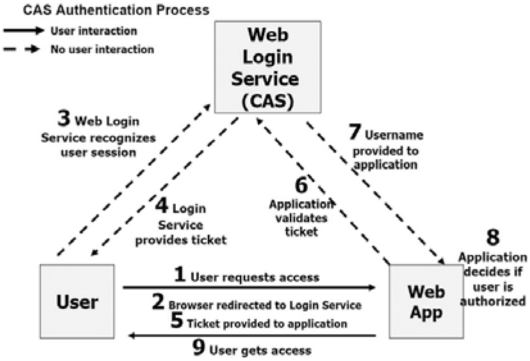
[Get your CERN Certificate]

In case of problems or questions please contact the HelpDesk:
Mail: helpdesk@cern.ch or Phone +41 22 76 78888

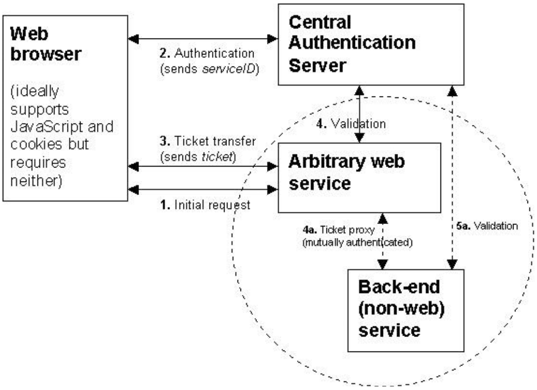
(Figure 15) Login Page in CERN Solution[7]

6.3 CAS(Central Authentication Service) Solution

The JA-SIG Central Authentication Service was originally developed by Yale University. It has since become a JA-SIG project. (Figure 17) shows CAS Architecture. It is designed as a standalone web application. It is currently implemented as several Java servlets and runs through the HTTPS server on secure.its.yale.edu. It is accessed through three URLs described below: the login URL, the validation URL, and the optional logout URL. [2-e] JA-SIG produces an enterprise-wide single sign on system known as CAS. As shown in (Figure 16), the Authentication has a simple method that returns the message, note that, in step 3, web login service recognizes user session, make sure it is safe, it is very important.


CAS Authentication Process
User interaction
No user interaction
Web Login Service (CAS)
3 Web Login Service recognizes user session
4 Login Service provides ticket
6 Application validates ticket
7 Username provided to application
8 Application decides if user is authorized
User
Web App
1 User requests access
2 Browser redirected to Login Service
5 Ticket provided to application
9 User gets access

(Figure 16) CAS Authentication Process[12]


Web browser
(ideally supports JavaScript and cookies but requires neither)
Central Authentication Server
2. Authentication (sends serviceID)
3. Ticket transfer (sends ticket)
1. Initial request
4. Validation
Arbitrary web service
4a. Ticket proxy (mutually authenticated)
5a. Validation
Back-end (non-web) service

(Figure 17) CAS Architecture with Arbitrary Web Service and back-end Service[2]

6.4 SAML (Security Assertion Markup Language) Solution

Security Assertion Markup Language (SAML) is an XML standard that allows secure web domains to exchange user authentication and authorization data. Using SAML, an online service provider can contact a separate online identity provider to authenticate users who are trying to access secure content.

(Figure 18) illustrates the steps of Logging in to Google Apps:

A. The user attempts to reach a hosted Google application, such as Gmail, Start Pages, or another Google service.

B. Google generates a SAML authentication request.

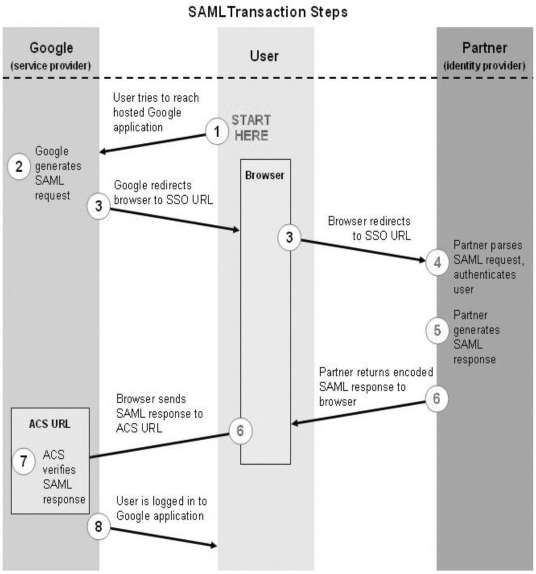
C. Google sends a redirect to the user's browser.

D. The partner generates a SAML response that contains the authenticated user's username.

E. The partner encodes the SAML response and the Relay State parameter and returns that information to the user's browser.

F. Google's ACS verifies the SAML response using the partner's public key.

G. The user has been redirected to the destination URL and is logged in to Google Apps.


SAMLTransaction Steps
Google
(service provider)
User
Partner
(identity provider)
User tries to reach hosted Google application
1
START HERE
2
Google generates SAML request
Browser
3
Google redirects browser to SSO URL
3
Browser redirects to SSO URL
4
Partner parses SAML request, authenticates user
5
Partner generates SAML response
6
Partner returns encoded SAML response to browser
ACS URL
Browser sends SAML response to ACS URL
6
7
ACS verifies SAML response
8
User is logged in to Google application

(Figure 18) Logging in to Google Apps using SAML[14]

7. Summary

In this paper, we surveyed SSO based security management including the knowledge domain of the area of cloud and its relevant components. Cloud computing refers to the delivery of software and other technology services over the Internet by a service provider. SSO refers to the ability to log on to a single security system once, rather than logging on separately to multiple security systems.

Existing SSO solutions in cloud computing environment suggest several methods. SSO-based security Issues illustrate these key items in cloud computing environment such as risks and security vulnerabilities of SSO. SSO supports for multiple and different domains in cloud computing environment.

Reference

[1] Intel Information Technology@, "Architecting Software as a Service for the Enterprise," Intel Inc., October 2009.

[2] CAS , http://www.jasig.org/cas.

[3] PingIdentity, http://www.pingidentity.com/.

[4] Hiroki Itoh and Teruko Miyata , "Standardization Trends in Identity anagement Technologies."Vol. 7 No. 6 June 2009.

[5] Juniper, "IDENTITY FED ERATION IN A HYBRID CLOUD COMPUTING ENVIRONMENT SOLUTION GUIDE," Juniper Inc., 2009.

[6] KEVIN JACKSON , "Secure Cloud

Computing: An Architecture Ontology Approach," Dataline Inc ., 2009.

[7] Mmanuel.Ormancey, "CERN Single Sign On solution," CERN Lab, 2009.

[8] cloud computing, http://www.wikinvest.com/concept/Cloud_Computing.

[9] PingIdentity, "single sign-on for SaaS Application," PingIdentity Inc., 2009.

[10] salesforce, http://www.salesforce.com/paas/.

[11] ikipedia, http://en.wikipedia.org/wiki/Infrastructure_as_a_service.

[12] CALPOLY, "Web Sign-On with CAS Happy Users, Developers," Security Officers SecureIT, 2006.

[13] Michael Morozov, http://blogs.neudesic.com/blogs/michael_morozov/archive/2006/03/17/72.aspx.

[14] Google, "SAML Single Sign-On (SSO) Service for Google Apps," Google Inc., 2006.

[15] Jeremy Beck, "What is Software as a Service (SaaS)," Scio Inc., January 2009.

[16] Cloudscaling, "Infrastructure-as-a-Service Builder's Guide," Cloudscaling Inc., 2009.

[17] ikipedia, http://en.wikipedia.org/wiki/Security_level_management.

[18] Dr. Jens Nimis, "Cloud Service Engineering," karlsruhe university., 2009.

[19] Theresa A. Thayer, "Security Access Control System Operations Manual," Ohio State University., 2008.

[20] John Stanford, "Practical Cloud Computing Patterns," Sunmicrosystems Inc., January 2009.

[21] Gary Ellison, "Security and Privacy Concerns of Internet Signal Sign On," Oracle Inc., 6 Sep 2002.

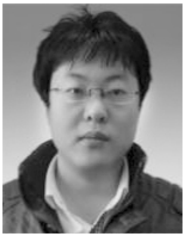
[22] SERL, "Security Issues in Cloud Computing," (SERL)Software Engineering Research Laboratory., 2008.

[23] J. Jeong et al., "Java-Based Single Sign-On Library Supporting SAML (Security Assertion Markup Language) for Distributed Web Services," Sejong University., 2008.

[24] Ecfirst, "SINGLE SIGN-ON (SSO) & IDENTITY MANAGEMENT-Assessment, Product Evaluation & Implementation," Ecfirst Inc., 2008.

[25] Workflow engine, http://en.wikipedia.org/wiki/Workflow_engine.

Authors



Jing Si Da

2007. Hustwb University, China (B.S.)
2008.~The Present, Pukyong National University(M.S.)
Research Interests : Artificial Intelligence,
Context-Awareness
E-mail : dadakingstar@hotmail.com

Youngmin Jung

2009. Pukyong National University(B.S.)
2009.~The Present, Pukyong National University(M.S.)
Research Interests : Security, Access Control, Cloud Computing
E-mail : jym1376@nate.com

Mokdong Chung

1981. Kyungpook National University(B.S.)
1983. Seoul National University(M.S.)
1990. Seoul National University(Ph.D.)
1984~1985. Goldstar Semiconductor Co, Research Scientist
1985~1996. Pusan University of Foreign Studies, Associate Professor
1999~2000. Iowa State University, Visiting Professor
1996~The Present, Pukyong National University, Professor
Research OOP technology, Computer Security for Application, Intelligent Agent, Context Aware Computing
E-mail : mdchung@pknu.ac.kr